United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. ***All entries must be Times New Roman, 12pt, and start on the next line.*** If you need further assistance, contact your LPO. A listing of the LPOs can be found here: https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: R05LAN (Region 5 Telework)	**System Owner: Rosalind Freeman**
Preparer: Aldwin Jereza	**Office: R05-MSD-HCB-LRS**
Date: 1/6/21	**Phone: 312-886-2911**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

System manages R5 telework applications.

The R5 Telework system is contained within the R05 Local Area Network General Support System (R05LAN). The system is a collection of forms related to managing and documenting telework forms at Region 5. These forms include telework applications/agreements and employee self-certification safety checklists.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and

define the collection of information by the system in question?

The Telework Enhancement Act of 2010 (December 9, 2010); Public Law 111–292.

Applies to Federal employees as defined by section 2105 of title 5 USC 6501.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes, March 2021.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

No.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

Employee Name • Employee Home Address(es)/Telework Location(s) • Employee Personal Phone Number • Type of Telework Agreement • Date of Signature/Activation • Date of Telework Training (if applicable) • Date of Expiration (if applicable) • Allowable Generic of Days of the Week an employee May use AWL (if applicable)

2.2 What are the sources of the information and how is the information collected for the system?

Data collection is initiated at the individual employee level (people) with electronic forms. Telework is a voluntary program, and employees must apply for it.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No

2.4 Discuss how accuracy of the data is ensured.

Expiration dates – if applicable – are included in the telework agreements and will be tracked based on compliance with internal EPA policy. Human Resources staff and supervisors will use expiration dates to reach out to employees to determine if another telework agreement is needed. Re-certification is required every 12 months.

Employees fill out the forms and sign and date them. After review, supervisors sign and date the form as well. After all signatures are completed, supervisor and employees have access to signed copies. Re-certification is required every 12 months.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Risk of collecting incorrect information or collecting more data than required.

Mitigation:

Forms are filled out directly by employees requesting to telework. Supervisors review for accuracy. A review is conducted annually to ensure information is correct.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes. System access rights are limited to employees and supervisors. Digital signatures ensure authenticity, integrity, and non-repudiation of the information on forms. Employees are able to input data for each telework application; Dual authentication (PIV card and LAN ID login) are required for all system users.

Yes, R05LAN has access control levels within the system. Employees are granted least privilege to the network. Signed forms are only accessible to employee and their supervisors. This is accomplished through granular network permissions.

User access and privileged access. User access is least privileged access which every employee has. It is issued via active directory during onboarding. Privileged access is limited to system administrators. There are several layers of review prior to getting privileged access to system.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Multifactor authentication is a requirement to log into system.

Access control to R05LAN is documented in the R05LAN GSS System Security Plan maintained in EPA's system repository (XACTA). R05LAN follows EPA Policy -

CIO 2150-P-07.2, Information Security - Identification and Authentication Procedure

3.3 Are there other components with assigned roles and responsibilities within the system?

No

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Only, internal, EPA staff will have access rights to the information. Employees and their supervisors have access to their own forms. Select Human Resources staff in Region 5 would have access upon request.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

The records schedule is 0039, Alternative Worksite Records (final 12/31/2013). This falls under NARA's general record schedule 1/42.
Records are kept in accordance with records schedule 0039. Approved applications are kept throughout employee's participation in the telework program up to 1 year after participation in the program. They are kept so employees and supervisors have a record of the telework agreement.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

- Retaining data for overly long duration
- Unauthorized individuals gaining access to PII
- Improper disposal of collected data

Mitigation:

- Unique ID and dual-factor authentication to R05LAN is enforced, access to telework

agreements is controlled through network permissions. These are accessible to only employee and supervisor.

- Record control schedules as applied to the records are a mitigating factor.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None, there is no external sharing.

Mitigation:

None.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in

Section 6.1?

The use of the data is relevant because it will ensure that all teleworking employees have completed the required paperwork and have received the required authorizations to telework.
Region 5 employees take annual Information Security and Privacy Awareness Training annually and agree to the EPA National Rules of Behavior. Multifactor authentication is required to gain access to the network and access to an employee's telework forms is only available to that employees and their supervisor.

R05LAN relies on user training to ensure that the information is used in accordance with the stated practices. In the event where a review is performed on using the "last accessed date" of the file, and it is identified neither the employee with the agreement nor their immediate supervisor accessed the file, an incident will be started and appropriate corrective taken. .

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

R5 Computer users are required to take the Information Security and Privacy Awareness training annually

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

- Unrecorded data changes.
- Users who do not have the proper training to protect PII are at risk of unauthorized disclosure and possible breach of data.

Mitigation:

- This risk is mitigated by the Active Directory control which prevent concurrent access to data files and record the last date changes were made.
- Users must take the mandatory ISPAT or have their access blocked.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

The information is for internal, Region 5 use only. The information will be used by employees, supervisors, and Human Resources for tracking purposes such as identification of the most current telework agreement(s) in place (employees can have multiple types of agreements for multiple workplace locations).

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes__ No_X__. If yes, what identifier(s) will be used.

(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

No, the data is not designed to be retrieved by personal identifier. The information is accessed via a secure shared folder, only accessible to the employee with the telework agreement and their immediate supervisor.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

R05LAN undergoes a 3rd party assessment in accordance with the information system life cycle requirements. Access to computers which store the forms are secured by multi-factor authentication. The information is stored as a non-editable PDF version of the original telework agreement in a secure shared folder, only accessible to the employee with the telework agreement and their immediate supervisor.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Individuals able to access PII could and use the data for unofficial/unauthorized purposes.

Mitigation:

PII stored in and transiting through the R05LAN is only viewable by specific EPA personnel with a need to know

- R05LAN GSS adheres to EPA access control policies
- Telework forms are only accessible to employee and their supervisor
- Multifactor authentication is required on R05LAN
- Users must take the mandatory ISPAT or have their access blocked.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Mitigation: